2018 / 5 / 17 — الموضوع: المحاضرة الأخيرة نظري

رمضان

ملاحظة تمرين: ناقش صحة القضية التالية:

إذا مسح d جميع قواسم n الموجبة فإن $\frac{n}{d}$ يمسح جميع هذه القواسم.

الحل: إذا كان d قاسم لـ n فإن

$$d \mid n \Rightarrow n = d \cdot d_1$$

$$\Rightarrow d_1 = \frac{n}{d}$$

وبالتالي إذا أخذ d جميع قواسم n فحتماً d_1 تمسح أيضاً جميع القواسم ومنه يكون:

$$\sum_{d \mid n} \varphi(d) = \sum_{\frac{n}{d} \mid n} \varphi\left(\frac{n}{d}\right)$$

مثال: $n = 12$

$$d \in \{1, 2, 3, 4, 6, 12\}$$

فإن القيم المقابلة $\frac{n}{d} \in \{12, 6, 4, 3, 2, 1\}$

مثال:
$n = 15$
$d \in \{1, 3, 5, 15\}$
$\frac{n}{d} \in \{15, 5, 3, 1\}$

مبرهنة: إذا كان $n \geq 1$ (عدد طبيعي) فإن:

$$n = \sum_{d \mid n} \varphi(d)$$

$$= \sum_{d \mid n} \varphi\left(\frac{n}{d}\right)$$

$\varphi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$
$\varphi(1) + \varphi(3) + \varphi(5) + \varphi(15)$
$1 + 2 + 4 + 8 = 15$

أي مجموع تم تابع أولر لقواسم العدد n الموجبة دائماً يساوي ذلك العدد n.

غير مطلوب الإثبات: نوزع الأعداد من 1 ← n

$1, 2, 3, 4, 5, 6 \ldots n$

d صفوف من النحو التالي:

$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15$

$S_3 = \{3, 6, 9, 12\}$ (قاسم مشترك لهم هو 3)

$S_5 = \{5, 10\}$ (قاسم مشترك لهم هو 5)

$S_1 = \{1\}$ $S_{15} = \{15\}$

أي أن S_d تتألف فقط تتألف من الأعداد m التي هي أصغر أو تساوي n وأكبر أو تساوي 1

$$1 \leq m \leq n$$

والتي قاسم الاشتراك لكل منها مع n يساوي d وإن عددها $\frac{\varphi(n)}{d}$

وبالتالي $d(m, n) = d$

هذا يعني أن

$$\left.\begin{matrix} n = n_0 d \\ m = m_0 d \end{matrix}\right\} \Rightarrow d(n_0, m_0) = 1$$

الموضوع:

أو بمعنى آخر: يقابل كل ثنائية لـ m ثنائية واحدة d وثنائية واحدة m_0، $m_0 = \frac{m}{d}$

لذا فإن عدد عناصر كل مجموعة من S_d يساوي عدد الأعداد الأولية نسبياً مع $n_0 = \frac{n}{d}$ والتي لا تتجاوز n_0 أي أن عدد عناصر عدد الأعداد الموجبة التي لا تتجاوز $S_d = \frac{n}{d}$ والأولية نسبياً معها.

$$|S_d| = \varphi\left(\frac{n}{d}\right)$$

أي أن عدد عناصرها.

ولما كان كل من الأعداد في هذه المجموعة ينتمي إلى صف واحد فقط: فإننا نجد أن:

$$n = \sum \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d)$$

الإثبات غير مطلوب

مثال بسيط:

$n = 10$ $\quad 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$

قواسم n هي: $\{1, 2, 5, 10\}$

ولنعرف المجموعات S_d:

$S_1 = \{m : d(m, 10) = 1 ; 1 \leq m \leq 10\}$
$= \{1, 3, 7, 9\}$

$S_2 = \{m : d(m, 10) = 2 ; 1 \leq m \leq 10\}$
$= \{2, 4, 6, 8\}$

$S_5 = \{m : d(m, 10) = 5 ; 1 \leq m \leq 10\}$
$= \{5\}$

$S_{10} = \{m : d(m, 10) = 1 ; 1 \leq m \leq 10\}$
$= \{10\}$

$|S_1| = 4$
$\varphi(\frac{10}{1}) = \varphi(10) = 4$
$|S_2| = 4$
$\varphi(\frac{10}{2}) = \varphi(5) = 4$
$|S_5| = 1$
$\varphi(\frac{10}{5}) = \varphi(2) = 1$
$|S_{10}| = 1$
$\varphi(\frac{10}{10}) = \varphi(1) = 1$

$\Rightarrow$ وعند ذلك يكون:

$\varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) = 10$

$1 + 4 + 4 + 4 = 10$

$10 = 10$

/ /

الموضوع:

الدالتان σ , τ :

تعريف الدالة τ : هي دالة حسابية قيمتها عند العدد n تساوي عدد القواسم الموجبة المختلفة للعدد n الصحيح الموجب.

$\tau(5) = 2$ قواسم 5 هي $\{1,5\}$

$\tau(4) = 3$ قواسم 4 هي $\{1,2,4\}$

$\tau(3) = 2$ $\{1,3\}$

$\tau(10) = 4$ $\{1,2,5,10\}$

$\tau(p) = 2$ وقواسم العدد p الأولي هي $\{1,p\}$ ، p أولي

ملاحظة: يمكن تعريف دالة τ

$$\tau(n) = \sum_{d|n} 1$$

(هنا تم جمع 1 مع عدد القواسم)

نبين هنا أن الدالة τ دالة ضربية :

الإثبات: إن الدالة $f(d) = 1$ أيا كانت $d \geq 1$ دالة ضربية تماما، لأن:

$$\left.\begin{array}{l} f(1) = 1 \\ f(d_1 d_2) = 1 \\ f(d_1) f(d_2) = 1.1 = 1 \end{array}\right\} \rightarrow f(d_1 d_2) = f(d_1) \cdot f(d_2)$$

لكن نعلم أنه إذا كانت $f(d)$ دالة ضربية فإن الدالة المعرفة على النحو التالي:

$$F(n) = \sum_{d|n} f(d)$$

دالة ضربية أيضا.

ومن ثم تكون الدالة المعرفة $\tau(n) = \sum_{d|n} 1$ دالة ضربية.

حساب الدالة τ :

نناقش: ① $n = p^{\alpha}$ ، p عدد أولي و $1 \leq \alpha$

فإن قواسم n الموجبة هي فقط هي: $1, p, p^2, \ldots, p^{\alpha-1}, p^{\alpha}$

وواضح أن عددها $\alpha+1$ أي

$$\boxed{\tau(p^{\alpha}) = \alpha+1}$$

(فقط بشوف القواسم ونعدها)

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

② إذا كانت العبارة القانونية لـ n هي:

$\tau(n) = (\alpha_1+1)(\alpha_2+1) \cdots (\alpha_k+1)$

فإن:

بما أن $p_1, p_2, \cdots p_k$ أولية نسبياً مثنى مثنى لأنها مختلفة، وهذا يعني أن $p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots p_k^{\alpha_k}$ أولية نسبياً مثنى مثنى، ولأن τ داله ضربية فسيكون:

$\tau(n) = \tau(p_1^{\alpha_1}) \cdot \tau(p_2^{\alpha_2}) \cdots \tau(p_k^{\alpha_k})$

$= (\alpha_1+1) \cdots (\alpha_k+1)$

أي:

$\tau(n) = \prod_{i=1}^{k} (\alpha_i+1)$

مثال:

$\tau(63) = \tau(3^2 \cdot 7^1)$

$= (2+1)(1+1) = 6$

قواسم 63 $\{1, 3, 7, 9, 21, 63\}$ عددها (6)

تعريف: تعريف الدالة σ: هي داله حسابية تقابل العدد الصحيح الموجب n بمجموع القواسم الموجبة المختلفة للعدد n.

مثال: قواسم (12) هي $\{1, 2, 3, 4, 6, 12\}$

$\tau(12) = 6$

$\tau(12) = \tau(2^2 3) = (2+1)(1+1) = 6$

$\sigma(12) = 1+2+3+4+6+12$

$= 28$

$\sigma(1) = 1$

$\sigma(2) = 3$

$\sigma(3) = 4$

$\sigma(4) = 1+2+4 = 7$

p أولي: $\sigma(p) = 1 + p$ | $\tau(p) = 2$

$\sigma(n) = \sum_{d|n} d = \sum_{d|n} f(d)$ و $f(d) = d$

وبسهولة يمكن البيان أن (σ) داله ضربية

/ /

الموضوع:

. اثبات أن σ دالة ضربية:

. حيث الدالة المعرفة بالعلاقة $f(d)=d$ لكل d في d دالة ضربية تماماً، حيث:

$$f(1)=1$$

$$f(d_1 \cdot d_2)=d_1 \cdot d_2 = f(d_1) \cdot f(d_2)$$

. فهي ضربية ومن ثم الدالة المقترنة مع النوع:

$$\sigma(n)=\sum_{d|n} d=\sum_{d|n} f(d)$$

ستكون دالة ضربية.

. حساب (σ(n)):

. نناقش حالتين: ① $n=p^{\alpha}$ و p أولي و $1\leq \alpha \in \mathbb{Z}$

إن قواسم $n=p^{\alpha}$ في موجبة هي بالضبط:

$$1, p, p^2, \text{---} \; p^{\alpha-1}, p^{\alpha}$$

ومن ثم:

$$\sigma(n)=1+p+p^2+ \text{--} \; p^{\alpha-1}+p^{\alpha}$$

. وهذه متسلسلة هندسية أساسها (p) وعدد حدودها (p^{α}) وحدها الأول (1)

. ومن ثم يكون مجموعها:

$$\sigma(n)=\frac{1-p^{\alpha+1}}{1-p} = \frac{p^{\alpha+1}-1}{p-1}$$

مجموع متسلسلة هندسية

② إذا كانت العبارة القانونية لـ n هي: $n=p_1^{\alpha_1} \cdot p_2^{\alpha_2} \text{---} \; p_k^{\alpha_k}$

فإن:

$$\sigma(n)=\prod_{i=1}^{k} \frac{p_i^{\alpha_i+1}-1}{p_i-1} = \prod \frac{1-p_i^{\alpha_i+1}}{1-p_i}$$

: $p_1^{\alpha_1}, p_2^{\alpha_2}, \text{---} \; p_k^{\alpha_k}$ أولية نسبياً مثنى مثنى:

$$\sigma(n)=\sigma(p_1^{\alpha_1}) \cdot \sigma(p_2^{\alpha_2}) \text{--} \; \sigma(p_k^{\alpha_k})$$

$$=\frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \text{---} \frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

بعض النماذج البسيطة:

① إذا كان p عدد أولي فإن

$$\sigma(p) = \frac{p^2-1}{p-1} = \frac{(p-1)(p+1)}{p-1} = p+1$$

②

180	2
90	2
45	3
15	3
5	5
1	

$180 = 2^2 \cdot 3^2 \cdot 5$

$$\sigma(180) = \sigma(2^2 \cdot 3^2 \cdot 5) = \frac{2^3-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1} = 7 \cdot 13 \cdot 6 = 546$$

$$\tau(180) = (\alpha_1+1)(\alpha_2+1)(\alpha_3+1) = (2+1)(2+1)(1+1) = 18$$

ملاحظة: إن الدالتين σ و τ ليستا ضربيتين تماماً، حيث:

$\tau(20) = \tau(2 \cdot 10)$ $\qquad \tau(2)\tau(10) = 2 \cdot 4 = 8$

$\tau(20) = \tau(2^2 5) = (2+1)(1+1) = 6$

أي أن $\tau(2 \cdot 10) \neq \tau(2) \cdot \tau(10)$

فلذلك τ ليست ضربية تماماً مع العلم أنها ضربية.

$$\sigma(20) = \sigma(2^2 \cdot 5) = \frac{2^3-1}{2-1} \cdot \frac{5^2-1}{5-1} = 7 \cdot 6 = 42$$

$$\sigma(2) \cdot \sigma(10) = 3 \cdot 18 = 54$$

غير متساويين σ ليست ضربية تماماً.

تعريف: حاصل ضرب القواسم الموجبة المختلفة للعدد $n>1$ يساوي $n^{\frac{\tau(n)}{2}}$

$$\prod_{d|n} d = (n)^{\frac{\tau(n)}{2}} = \sqrt{n^{\tau(n)}}$$

/ /

الموضوع:

الإثبات: إذا كان d قاسماً لـ n فإن $n=d.d'$ ،

ولما كان عدد القواسم الموجبة لـ n تساوي $\tau(n)$

ومن ثم يكون لدينا عدد من العلاقات من هذا النوع $n=d.d'$ يساوي $\tau(n)$

بضرب هذه العلاقات

$$n^{\tau(n)} = \prod_{d|n} d \cdot \prod_{d'|n} d' \quad (*)$$

حيث d يقسم n و d' يقسم n.

ولكن إذا تمسح d جميع قواسم n فإن d' تمسح أيضاً جميع قواسم n

أي أن: $\prod_{d'|n} d' = \prod_{d|n} d$ وبالتالي هذه العلاقة * تكتب:

$$n^{\tau(n)} = \left(\prod_{d|n} d\right)^2 \Rightarrow \prod_{d|n} d = \sqrt{n^{\tau(n)}} = n^{\frac{\tau(n)}{2}}$$

مثل $n=10$

$1, 2, 5, 10$

$10 = 1.10$
$= 2.5$
$= 10.1$
$= 5.2$

تمرين بسيط: اثبت أن

$$\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d} \quad \text{أي} \quad \sigma(n) = n \cdot \sum_{d|n} \frac{1}{d}$$

الإثبات: بالتعريف إن: $\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d}$

ولكن جميع قواسم n الموجبة هي:

$d_1, d_2, \ldots, d_k$

فعندئذ: [illegible] $\sigma(n) = \frac{n}{d_1} + \frac{n}{d_2} + \cdots \frac{n}{d_k}$

$$= n\left(\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k}\right)$$

$$\sigma(n) = n \cdot \sum_{d|n} \frac{1}{d}$$

تمرين أخير: أوجد العدد الصحيح n الذي يحقق العلاقة الآتية:
$\tau(10n) = 10$

الحل:

$10 = 2.5$

فهو جداء عددين أوليين لذا فإن $10n$ يلزم أن يكون ما يشكل
$10n = 2^{\alpha} \cdot 5^{\beta}$

ولذا يكون: $\tau(10n) = (\alpha+1)(\beta+1) = 10 = 2.5$

ومنه: إما أن $\alpha+1=2$ و $\beta+1=5$
فعندئذ: $\alpha_1=1$; $\beta=4$

$\Rightarrow 10n=2^1\cdot 5^4$
$\Rightarrow n=5^3=125$

أو

$\left.\begin{array}{l}\alpha+1=5\\ \beta+1=2\end{array}\right\} \Rightarrow \beta=1$, $\alpha=4$

$10n=2^4\cdot 5^1 \Rightarrow n=2^3=8$

تعريف: نقول عن العدد الصحيح n أنه كامل أو تام إذا كان $\sigma(n)=2n$

أصغر عددين كاملين معلومين:
$n=6 \Rightarrow \sigma(6)=12$
$\sigma(6)=2\cdot 6$
$n=28 \Rightarrow \sigma(28)=2\cdot 28=56$

- يقال عن العدد أنه زائد إذا كان $\sigma(n)>2n$

- ويقال أنه ناقص إذا كان $\sigma(n)<2n$

- ويقال أن العددين n و m متحابان إذا كان:
$\sigma(n)=\sigma(m)=n+m$
إن العددين 284 و 220 عددان متحابان.

وجد العلماء عدداً من الأعداد الكاملة (تامة) وكلها زوجية ولكن إلى الآن تبقى أنه مفتوحة لا يوجد عدد كامل فردي.
- تسمى الأعداد من الشكل
$M_k=2^k-1$ و $k\geq 2$ أعداد ميرسين (Mersenne Numbers)

- وتدعى الأعداد الأولية ذات الشكل

$M_p = 2^2 - 1$ من الأوليات ميرسين.

- نعرف دالة موبياس :

$$\mu(n) = \begin{cases} 1 & ; n = 1 \\ 0 & ; \text{إذا قبل العدد } n \text{ القسمة على } p^2 \text{ حيث } p \text{ أولي } \quad p^2 \mid n \\ (-1)^r & ; n = p_1 \cdot p_2 \cdots p_r \end{cases}$$

مثال

$30 = 2 \cdot 3 \cdot 5$

$\mu(30) = (-1)^3 = -1$

$\mu(10) = \mu(2 \cdot 5) = (-1)^2 = 1$

$\mu(12) = \mu(2^2 \cdot 3) = 0$

يبرهن أن موبياس دالة جزئية.

بينما دالة ليوفيل λ

$$\lambda(n) = \begin{cases} 1 & ; n = 1 \\ (-1)^{\alpha_1 + \alpha_2 + \cdots + \alpha_r} & ; n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \end{cases}$$

نهاية البحث

دالة موبياس ودالة ليوفيل
غير مطلوبين بالامتحان
فقط للاطلاع

/ /

الموضوع: ~~الفصل الرابع والأخير~~

الجذور الأولية والأدلة

تعريف رتبة العنصر

المرتبة: إن رتبة العنصر a بالمقاس m أو الأس الذي ينتمي إليه العدد الصحيح a للمقاس m) حيث $d(a,m)=1$ هي أصغر عدد صحيح موجب $k \neq 0$ يحقق الشرط:

$$a^k \equiv 1 \pmod m$$

ويقال عندئذ إن k هو دليل أولي أو دليل العدد a بالمقاس m) ويكتب:

رتبة $ord_m a$ — $k = Ind_m a$ أو $Ind\ a \pmod m$

مثال: ما هي رتبة 2 بالمقاس 7

$$2^2 \equiv 4 \pmod 7$$

$$2^3 \equiv 1 \pmod 7$$

أي أن رتبة 2 للمقاس 7 تساوي 3

$ord_7 2 = 3$ و $ord_6 5 = 2 \leftarrow$ $5^2 \equiv 1 \pmod 6$

$$ord_{14} 3 = 6$$

$$3^2 \equiv 9 \pmod{14}$$

$$3^3 \equiv 13 \pmod{14}$$

$$3^4 \equiv 11 \pmod{14}$$

$\vdots$

$$3^6 \equiv 1 \pmod{14}$$

دورة **مبرهنة**: إذا كانت مرتبة أو رتبة العدد الصحيح a للمقاس m تساوي k

فإن $k \mid s \Leftrightarrow a^s \equiv 1 \pmod m$

البرهان: $\Rightarrow$ إذا كان $k \mid s$ فإن $s = k \cdot k_1$ ومن ثم:

$$a^s = (a^k)^{k_1} \equiv (1)^{k_1} \bmod m \equiv 1 \pmod m$$

إذا كان s عدداً صحيحاً بحيث $a^s \equiv 1 \pmod m$ كيف هذا التطابق فحسب خوارزمية القسمة حيث:

$$s = q \cdot k + r \quad ، \quad 0 \leq r < k$$

وبالتالي $a^s = (a^k)^q \cdot a^r \equiv 1 \pmod{m}$

$\Rightarrow a^r \equiv 1 \pmod{m}$

وحسب تعريف المرتبة لأن k أصغر عدد صحيح موجب يحقق هذا التطابق يجب أن يكون $\boxed{r=0}$ وعندئذ $s = q \cdot k$ أي $k \mid s$

نتيجة: إذا كانت k رتبة a بالمقاس m فإن k حتماً تقسم $\varphi(m)$ $k \mid \varphi(m)$

وتم أن مبرهنة أولر $a^{\varphi(m)} \equiv 1 \pmod{m}$

إذا كان $d \mid (a,m) = 1$ حسب المبرهنة السابقة يجب أن تكون

$k \mid \varphi(m)$

$k = ord_m a$

لبحث عن مرتبة a للمقاس m يكفي أن نبحث بين قواسم $\varphi(m)$ حيث $\varphi(m)$ هو عدد الأعداد الأولية النسبية مع m موجبة وأصغر من m.

مثال: إذا أردنا أن نبحث عن $ord_{13} 2$

[1] نوجد $\varphi(13)$: $\varphi(13) = 12$

قواسم [12] $\{1, 2, 3, 4, 6, 12\}$

$2^2 \equiv 4 \pmod{13}$

$2^3 \equiv 8 \pmod{13}$

$2^4 \equiv 3 \pmod{13}$

$2^6 \equiv 12 \pmod{13}$

$2^{12} \equiv 1 \pmod{13}$ $\quad a^{\varphi(m)} = 1$

$ord_{13} 2 = 12 = \varphi(3)$

لذلك يقال عن شيء كهذا (2) أنه جذر أولي أو أصلي للعدد (13) وبشكل عام نقول عن العدد a أنه جذر أولي للقياس m إذا وفقط إذا كانت:

$$ord_m a = \varphi(m)$$

السؤال بيّن إذا كان العدد ( ) جذر أولي أو غير جذر أولي.

مبرهنة: إذا كانت رتبة a للقياس m تساوي K $\quad ord_m a = k$

فإن $a^t \equiv a^s (mod\ m)$

إذا وفقط إذا: $t \equiv s (mod\ k)$

الإثبات: $\Leftarrow$ نفرض أولاً أن $a^t \equiv a^s (mod\ m)$

نفرض أن $t \geq s$

وما دام $d(a,m)=1$ فيمكن الاختصار على a^s ويكون:

$a^{t-s} \equiv 1 (mod\ m)$

حسب المبرهنة ① $\quad K \mid (t-s)$

$\Rightarrow t \equiv s (mod\ k)$

$\Rightightarrow$ نفرض أن $t \equiv s (mod\ k)$، لنثبت أن $a^t \equiv a^s (mod\ m)$

حسب خوارزمية القسمة $K \mid (t-s)$

$t = kq + s$

ومن ثم:

$$a^t = (a^k)^q \cdot a^s \equiv a^s (mod\ m)$$

نتيجة: ① إذا كانت رتبة a بالقياس m هي k $\quad ord_m a = k$

فإن الأعداد $a = a^2, a^3, \ldots a^{k-1}, a^k$

تكون غير متطابقة بالقياس m

② إذا كانت رتبة a بالقياس m هي k $\quad ord_m a = k$

فإن رتبة

$$ord_m a^s = \frac{ord_m a}{d(k,s)}$$

/ /

الموضوع:

مبرهنة: دون برهان إذا وجد جذر أولي للعدد m وكان هذا الجذر هو a
أي أن $ord_m a = \varphi(m)$
فإن العدد m يوجد $\varphi(\varphi(m))$ جذراً أولياً.

مثال: إذا كان p عدداً أولياً و r جذراً أولياً للعدد p أي أن
$ord_p r = p-1$
فإن عدد الجذور الأولية للعدد p هو $\varphi(p-1)$

مثال: إذا كان p=7 فإن $\varphi(7)=6$ و $\varphi(6)=2$ (عدد الأعداد الأولية مع 6 وأصغر منها)
ومن ثم للعدد 7 جذران أوليان هما 3 و 5
تأكد بالبيت

نهاية المحاضرة

❤ وخلصنا المقرر ❤